(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 061 482 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
20.12.2000 Bulletin 2000/51

(51) Int. Cl.^{7}: **G07F 7/10**

(21) Application number: **00202089.9**

(22) Date of filing: **16.06.2000**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **18.06.1999 US 139732 P**

(71) Applicant:
Citicorp Development Center, Inc.
Los Angeles, California 90066 (US)

(72) Inventors:
- **DO, Cuong D.**
  RESEDA, CA 91335 (US)
- **RIZZO, Carol J.**
  LIVINGSTON, NJ 07039 (US)
- **WILLIAMS, Leon**
  SUMMIT, NJ 07901 (US)

(74) Representative: **Hynell, Magnus**
Hynell Patenttjänst AB,
Patron Carls väg 2
683 40 Hagfors/Uddeholm (SE)

(54) Method, system, and apparatus for transmitting, receiving, and displaying information

(57) An augmented personal digital assistant (PDA), or alternatively a personal financial assistant (PFA) having magnetic and smart card reading/writing features, financial software, biometric verification features, timed information removal features, and automatic communications capabilities to interface with automated teller machines (ATMs) or other PDAs. The device further includes a radio frequency (RF) transceiver, an infrared data association (IRDA) transceiver, data encryption standard (DES) processor and flash memory. Optional hardware includes biometrics hardware and an RSA chip.

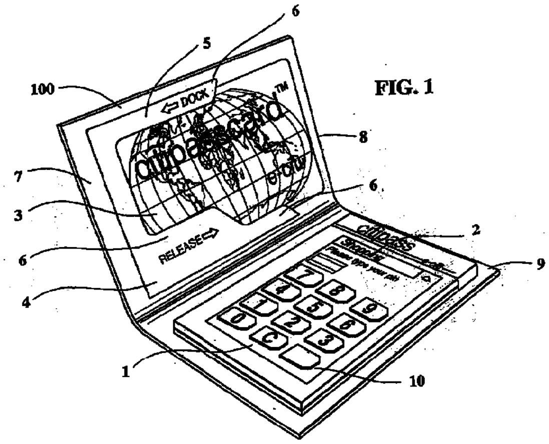


FIG. 1

Printed by Xerox (UK) Business Services
2.16.7 (HRS)/3.6

Description

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application claims priority to, and herein incorporates by reference, applicants' copending U.S. Provisional Application No. 60/139,732 filed June 18, 1999.

BACKGROUND OF THE INVENTION

[0002] The present invention relates generally to methods, systems, and devices for transmitting, receiving, and displaying information. More specifically, one embodiment of the present invention is an augmented personal digital assistant (PDA), or alternatively a personal financial assistant (PFA) having magnetic and smart card reading/writing features, financial software, biometric verification features, timed information removal features, and automatic communications capabilities to interface with other PDAs or automated teller machines (ATMs).

[0003] In many circumstances, the ability to access information and utilize financial services is dependent upon the ability to carry multiple cards, such as credit and debit cards. These cards may take the form of magnetic stripe cards or smart cards. There are, however, several problems with consumers carrying numerous cards. These cards add weight and bulk to a consumer's wallet or purse, and present increased opportunities for loss or theft. As a result, consumers may limit the numbers of card accounts they maintain, thereby limiting potential business opportunities for financial services providers.

[0004] Additionally, these cards generally have expiration dates, making it necessary for routine replacement. This leads to a two-fold problem, first, consumers may forget to replace an expired card, and, second, card providers must routinely reissue new cards. Significant costs are incurred in the administration and replacement of these cards.

[0005] Not only is there a problem with the number of cards necessary to access various services; increasingly, people are carrying electronic organizers, laptop computers, cellular telephones, and other microcomputer based devices. These devices have become indispensable tools for many people. Accordingly, there is a need for an effective method, system, and device that consolidate financial services cards with microcomputer based devices.

SUMMARY OF THE INVENTION

[0006] The above identified shortcomings are overcome by the present invention, which relates to a universal card system with an integrated PDA/PFA (hereinafter referred to as "the device" of the present invention). The device includes all known features of a pocket PDA, and additionally includes card reading/writing capabilities, timed information removal features, biometric verification tools, wireless transmission features, automatic transmission of information, and e-commerce and banking software.

[0007] The present invention benefits both the consumer, as well as, financial services providers. The consumer benefits by the reduction in the number of cards to be carried, improved security, consolidation of personal financial information, and access to a banking network. Consolidation results because the user will have a personal identification number (PIN) in which to program the universal card into a desired credit card, debit card, charge card etc. Further, security is enhanced because the data encoded on the universal card erases after a preset period and/or on demand, thereby returning the universal card into its generic status after a transaction.

[0008] The consolidation of financial information is further enhanced because, for example, all credit, charge, and debit card information, as well as, electronic receipts and transaction statements are stored on a single device, and may be displayed and downloaded. Because of the considerable banking services provided by the pocket-sized device, the invention can essentially be viewed as a "Bank in Pocket" device.

[0009] An embodiment of the invention provides for the use of the device to access electronic data and services through long range, omni directional RF transmission, as well as, shorter range, unidirectional IRDA transmission. Infrared transmission in the present invention, for example, allows the user of the device to establish a two-way IRDA link with a home personal computer (PC), thereby uploading data onto the home PC database, as well as, downloading data onto the device.

[0010] The financial services provider associated with the present invention benefits because there will be fewer physical cards issued, and transactional information is made available to consumers in electronic form. Security is also enhanced and a precise audit trail can be established. Further, the invention may serve as an open platform between financial institutions.

[0011] The basic hardware of an embodiment of the present invention includes a central processing unit (CPU) and memory connected to a battery, a display, a user interface, an RF transceiver, an IRDA transceiver, a data encryption standard (DES) processor, and flash memory. The embodiment also includes biometrics hardware and a Rivest, Shamir, Adelman (RSA) encryption chip, as well as, a card encoding capability.

[0012] Although the embodiments shown depict a highly portable device, the present invention is not restricted to a handheld configuration. The present invention may be incorporated as part of a personal computer. Additionally, the present invention may be permanently installed as part of a system to serve individuals located in a certain location, such as at a kiosk, in a car, on board an aircraft, or other conveyance.

[0013] Data input may be performed via a keypad, a touch screen, or a stylus, as well as, through speech recognition. The present invention can incorporate a combination of these data input features. Furthermore, an embodiment provides wireless Internet access capability. The screen and the keypad of one embodiment is oriented in a side-by-side configuration. A protective shell or cover supports and protects the device in a manner not to interfere with data transmissions. An embodiment of the present invention also includes features of a portable cellular phone or pager, or a combination thereof, making the device a unitary item so that consumers may carry a single, multi-purpose piece of hardware.

[0014] The ability to access information contained in the present invention is determined by the authorized user of the device. Access to different types of information stored on or received through the device may be varied. Certain information may be made available to anybody who comes in contact with the device. For example, medical personnel may have immediate access to the user's medical/health information. In one embodiment, a special emergency key is included on the device to make it easy for medical personnel to retrieve the user's medical/health information.

[0015] Another embodiment allows for the automatic transmission of information. This provides the advantage of enhanced customer service. For example, if a bank customer and bank are both utilizing an embodiment of the inventive system, the bank teller may automatically have the customer's information displayed as the customer approaches. This allows the teller to greet the customer by name and also, for example, preview the customer's account information.

[0016] Further, by using the IRDA or RF transceiver, a user may pre-program a transaction, for example, the withdrawal of money from an ATM so that the user does not have to wait to enter all the transaction information while physically at the ATM. In this embodiment, as the user approaches an "on-us" ATM, even while in a car, for example, the RF or IRDA transmission allows the ATM to receive, and temporarily store, the user's information. Then, as the user approaches the ATM, a biometrics verification process matches transmitted biometric data from the device with the observed characteristics of the user and, upon satisfactory verification, automatically processes the user's pre-programmed transaction. After this transaction is completed, a receipt is electronically transferred to the device, eliminating the need for a paper receipt and further increasing the speed and security of such transactions. Further, the invention allows financial institutions to more quickly and effectively tailor information to specific individuals.

[0017] A variety of information is stored in the device. Some examples include information regarding credit card accounts, checking accounts, savings accounts, health insurance, frequent flyer awards, safe deposit box identification, telephone calling card accounts, and driver's license information. Other types of information may also be stored using the present invention.

[0018] An embodiment utilizes both magnetic stripe cards, as well as, smart cards as the universal card. Although there has been a lot of movement towards smart cards, magnetic stripe cards will continue to be utilized as long as the vast magnetic stripe infrastructure continues to exists. An object of the present invention is to allow users access to existing, as well as emerging technologies.

[0019] The present invention has a number of security features. An embodiment has a data encryption standard processor having a fixed internal unreadable key, as well as an RSA chip for public key encryption. A personal identification number (PIN) may be selected and entered by the user of the present invention. Additionally, card identification numbers (CINs) are assigned to various cards belonging to the user. For added security, biometrics data is stored in the present invention, to further ensure that only authorized users are able to use the device. This may include fingerprint, thumbprint, palm print, or an IrisCode. Furthermore, the device erases information added to the universal cards upon user initiation or after a predetermined time interval.

[0020] Banking with the present invention may be conducted from a user's home, either with or without a personal computer. By installing a low cost RF modem between the user's home phone and the wall jack, a user may access his/her home banking network. Point of sale transactions may also be performed with the device, either with a universal card or through wireless transmission. For point of sale transactions, the user would enter a PIN and use the device to select the card he/she wishes to use for the purchase. The device would then write the necessary information onto the universal card. The universal card would then be swiped through a point of sale terminal that is connected to a point of service network. The transaction would then proceed and the purchase would be completed.

[0021] For wireless point of sale transactions, the data stored in the device would be transmitted wirelessly via an RF or IRDA transceiver to an RF or IRDA modem at the point of sale, the modem being connected to a point of sale network.

[0022] One embodiment of the device comprises a user interface for receiving input from a user to initiate an information exchange; a power source for providing power to enable standalone operation of said device; a central processing unit operatively connected to said user interface for controlling the operation of said device; a memory component operatively connected to said central processing unit, for storing information and software; an encryption/decryption processor for enabling encryption/decryption of data transmitted via a wireless data transmission; a communications module enabling, without said user's prompt, said wireless data transmission between said device and a terminal when said device is within a communications range of said terminal; and wherein said communications module wirelessly transmits verification information associated with an authorized user of said device to enable verification of whether said user of said device is said authorized user.

[0023] An embodiment of the inventive system comprises a portable communications device; a card reader/writer associated with said portable communications device; a universal card wherein data is written and retrieved from said card with said card reader/writer, and wherein data is automatically erased from said card at a timed interval; a biometric identifier for verifying a user of said portable communications device; and an information terminal for automatic data transmission with said portable communications device when said portable communications device is within a communications range with said information terminal.

[0024] Another embodiment of the system comprises a device with a user interface for receiving input from a user to initiate an information exchange; a power source for providing power to enable standalone operation of said device; a central processing unit operatively connected to said user interface for controlling the operation of said device; a memory component operatively connected to said central processing unit, for storing information and software; an encryption/decryption processor within the device for enabling encryption/decryption of data transmitted via a wireless data transmission; a terminal for communicating with said device; a communications module enabling, without said user's prompt, said wireless data transmission between said device and said terminal when said device is within a communications range of said terminal; and wherein said communications module wirelessly transmits verification information associated with an authorized user of said device to enable said terminal to verify whether said user of said device is said authorized user.

[0025] A further embodiment of the present invention is a method for performing an electronic transaction with an information and transaction processing system, comprising receiving transactional information from a device; receiving verification information from said device; verifying a user of said device corresponds with said verification information; and transmitting and receiving data automatically with said device when said device is within a predetermined communications range.

[0026] Further aspects and advantages of the present invention will be more clearly apparent to those skilled in the art during the course of the following description, references being made to the accompanying drawings which illustrate some embodiments of the present invention and wherein like characters of reference designate like parts throughout the drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0027]

FIGURE 1 is a perspective view of one embodiment of the present invention;

FIGURE 2 is a perspective view of another embodiment of the present invention;

FIGURE 3 is a perspective view of another embodiment of the present invention;

FIGURE 4 is a block diagram showing the basic hardware and optional hardware of one embodiment of the present invention;

FIGURE 5 is a diagram illustrating the enrollment of a new user;

FIGURE 6 is a diagram illustrating the interaction between one embodiment of the present invention with an "on-us" ATM, shared network ATM, and POS terminal;

FIGURE 7 is a diagram further illustrating the interaction between one embodiment of the present invention and an "on-us" ATM;

FIGURE 8 is a diagram further illustrating the interaction between one embodiment of the present invention and a shared network ATM;

FIGURE 9 is a diagram further illustrating the interaction between one embodiment of the present invention and a POS terminal;

FIGURE 10 is a diagram illustrating the interaction between one embodiment of the present invention and a POS terminal in a passive mode;

FIGURE 11 is a diagram illustrating the interaction between one embodiment of the present invention and a home banking network;

FIGURE 12 is a diagram illustrating the interaction between one embodiment of the present invention and a personal computer; and

FIGURE 13 is a diagram illustrating the an information updating embodiment of the present invention.

DETAILED DESCRIPTION OF A PREFERRED EMBODIMENT

[0028] For the purposes of promoting an understanding of the principles of the invention, references will now be made to several embodiments of the present invention as illustrated in **FIGURES 1-13**. It will be understood that no limitation of the scope of the invention is thereby intended. The terminology used herein is for the purpose of description and not limitation. Any modifications or variations in the depicted method, system, or device, and such further applications of the principles of the invention as illustrated therein, as would normally occur to one skilled in the art, are considered to be within the spirit of this invention. For instance, features illustrated or described as part of one embodiment can be used on another embodiment to yield a still further embodiment. Thus, it is intended that the present invention cover such modifications and variations that come within the scope of the appended claims and their equivalents.

[0029] Referring now to **FIGURE 1**, there is shown a perspective view of one embodiment of the device **100** of the present invention. The device **100** has a user interface **1** and display **2**. The user interface **1** shown is a keypad. Alternate embodiments include a touch screen interface/display. Also shown is universal card **3** as seen when stored in a card reader/writer **4**. The card reader/writer **4** includes a docking port **5** with lips **6** to hold the universal card **3**. The lips **6** are adjacent to the top and bottom portion of the card. Protective cover **7** is shown supporting and protecting the device **100** so as not to interfere with any data transmissions. The protective cover **7** is segmented by two panels **8** and **9**. The interface includes an emergency key **10** that provides medical and/or contact information. Another embodiment provides for emergency communication with a third party via cellular telephone. The information accessed via the emergency key **10** is preauthorized by the authorized user for access by others.

[0030] Referring now to **FIGURE 2**, there is shown a perspective view of another embodiment of the device **200**. In this embodiment, the protective cover **18** has three panels with the docking port located on the top panel **8**, the display on the center panel **11**, and the primary interface located on the lower panel **12**. The display **13** is a liquid crystal display (LCD). User interface is located on panels **11** and **12**. The alpha-numeric keypad **14** is located on the lower panel **12**, with the scrolling arrows **15** and **16** and an enter key **17** located on the center panel **11**. Again, universal card **3** is shown stored in the docked position in the card reader/writer **4**.

[0031] Referring now to **FIGURE 3**, an embodiment of the device **300** is shown without the card reading/writing feature. The protective cover **19** has two panels **20** and **21**. The primary interface **22** is located on the lower panel **21**. The display/interface **23** is located on the upper panel **20**. The display/interface **23** being an LCD, allowing for data entry with a stylus. As is evident in **FIGURE 3**, the embodiments in **FIGURE 1** and **FIGURE 2** do not require card reading/writing features to perform other functions, for example encrypted wireless data transmission.

[0032] Referring now to **FIGURE 4**, there is shown a block diagram displaying the basic hardware, and some optional hardware, of one embodiment of the present invention. The basic hardware of the present invention includes a central processing unit (CPU) and memory device **24**. CPU **24** is operatively connected to battery **25**, display **26**, user interface **27**, RF transceiver **28**, and IRDA transceiver **29**. Also operatively connected to CPU **24** is data encryption standard (DES) processor **30** and flash memory **31**. There is also some optional hardware that may be operatively connected to CPU **24**, including, but not limited to, biometrics hardware **32** and RSA chip **33**.

[0033] CPU **24** controls the present invention by executing programs stored within its memory. Display **26** may be any type and size of the various data/command displays available, and is preferably a liquid crystal display (LCD) having graphics capabilities. User interface **27** may be any type of user-friendly interface for data/command entry such as a stylus, touch screen, speech recognition, or other data entry systems. User interface **27** may also be incorporated into display **26**, instead of being separate from display **26**. RF transceiver **28** is a radio frequency transceiver capable of two-way data transfer between the device and an ATM, a bank teller station, other PDAs, or a greeting station; and is preferably a wireless RF transceiver with a ten meter omni-directional range. IRDA transceiver **29** is an infrared optical data transceiver capable of short range infrared communication with other infrared devices, such as PDAs and personal computers for data uploading and downloading, the IRDA transceiver preferably having a one meter directional range.

[0034] DES processor **30** is included for security purposes. DES processor **30** utilizes a symmetric-key encryption method and is preferably a 56 bit encryption processor containing a fixed internal unreadable key. A triple DES is provided for additional security. RSA chip **33** is for performing public key encryption.

[0035] The flash memory **31** is for storing data and programs for easier updating. Biometrics hardware **32** may be any conventional type of biometrics hardware capable of storing encrypted personal authenticating information such as a user's fingerprint, thumbprint, palm print, IrisCode or combination thereof. Biometrics hardware **32** is included as a security measure to supplement the personal identification number (PIN), terminal identification number (TIN) and card identification number (CIN) security code systems of the present invention. In one embodiment, the biometrics hardware **32** stores an enrolled personal IrisCode (512 Bytes) in encrypted mode.

[0036] **FIGURE 5** is a chart showing an embodiment of a method for activating the present system upon enrollment of a new user **34**. The user is assigned a personal identification number (PIN) **35** that is used by the user at the time of a transaction for identification. The card account and banking account information **36** of the user is entered onto the device through data transmission or manual input. The various card accounts, for example, Visa™, MasterCard™, Diners Club™, are identified by a card identification number (CIN). Likewise, banking account information, for example, checking accounts, savings accounts, CDs, and business checking accounts, are identified by an account number. Further, information **36**, such as, medical information, safe deposit box identification, frequent flier information, and insurance policy information may be entered. During the transaction, the user's iris image **37** is captured by a camera and compared to the transmitted IrisCode. The network **38** recognizes the terminals by the terminal identification number (TIN) and indexes the TIN for IrisCode searching/matching. The user's **39** IrisCode is stored in an encrypted mode and verified within two feet of a transaction terminal.

[0037] Referring now to **FIGURE 6**, there is shown an overall system illustrating the interaction between device **200**, which may also be embodiment **100** or **300**, and associated "on-us" ATM **40**, as well as, and shared network ATM **41** and POS terminal **42**. In an embodiment of the "on-us" transaction shown in more detail in **FIGURE 7**, a user pre-programs a desired transaction **43** into the memory of device **200**. For example, the user may preset the transaction at home. As the user approaches the ATM, in one embodiment, at a point within 10 meters for RF transmission, the user's stored information **43** is transmitted automatically (when in an automatic mode) or is transmitted upon user initiation to an "on-us" ATM **40** to begin a transaction. The stored information **43** including CIN, PIN, TIN, and IrisCode, along with the pre-programmed transaction request, is transmitted to the ATM. The transmission can be via either IRDA or RF, or other transmission systems, such as, transponder systems. The user's information **43** is received by the ATM **40** via a transceiver. The ATM verifies the transmitted TIN/PIN/CIN with the ATM's network servers **44A** and **44B**. In this embodiment, a camera **45**, for example a Sensar Inc. camera, at the ATM captures the iris image **46** of the user and verifies it with the encrypted IrisCode **43** transmitted to the ATM **40**. Once the transaction is authorized, for example, a cash withdrawal transaction **47**, the user takes the cash and receives a wireless download of the transaction record **48** via RF. The device will receive the download even if it is in the user's pocket. Many different types of transactions may be performed, including deposits **49** made by the user into an account.

[0038] Alternatively, in an shared network transaction, shown in **FIGURE 8**, device **200** may be used to write to a universal **3** magnetic stripe or a smartcard, which can then be used at a card reader at shared network ATM **41**. The user begins by entering the PIN **50** for verifying user's access to the device **200**. The device **200** is used to select **51** which of the several card formats stored in memory the user wishes to use for the given transaction. The selected card information is then written onto the universal card **3** via card reader/writer **4**. Universal card **3** then acts as the selected card for a typical transaction at, for example, a shared network ATM **41** or POS terminal. The encoded universal card is entered into the ATM **41**. The ATM verifies the PIN with the ATM's servers **52A** and **52B**. Once the transaction, for example, a cash withdrawal **47**, is authorized, the user takes the cash and receives a transaction record **53** via display or traditional paper receipt.

[0039] When the universal card **3** is embodied as a smart card, the card erases the encoded data after a specified duration, for example, ten minutes. With the universal card **3** embodied as a magnetic stripe card, the device erases the data from the card once the card has been docked and/or after a specified time interval.

[0040] In **FIGURE 9**, a POS transaction is shown in further detail. For example, a user desires to make a purchase at a store. The user enters the PIN **50** for verifying user's access to the device **200**. The user selects **51** the type of credit card account with which to make the purchase. The universal card is encoded as the desired credit card **3B**, and the card is processed at a POS terminal **42** which is connected via a phone line **54** to a POS network **55**. The POS terminal **42** displays whether the transaction is authorized.

[0041] In **FIGURE 10**, a transaction is illustrated wherein the POS terminal **42** is in a passive mode. In this embodiment, the user again enters the PIN **50** for verifying user's access to the device **200**. The user selects **51** the type of credit card account with which to make the purchase. An RF modem **56** is linked with the POS network **55**. The device **200** is used to transmit via RF the selected transaction to the RF modem **56**. The transaction is checked for authorization and processed. A transaction record is then transmitted via RF to the device **200**.

[0042] Referring now to **FIGURE 11**, there is shown a diagram illustrating the interaction between device **200** and home banking network **57**. In this embodiment, information is transferred to and from device **200** through RF modem **56** which is connected via phone **58** and phone line to a home banking network **57**. The RF modem **56** may be a low cost modem installed on the home phone line. Accordingly, the user can wirelessly access the home banking network, and the network can download account information onto the device **200**.

[0043] As shown in **FIGURE 12** information may also be transferred between device **200** and personal computer **59**. In this example, data transmission is via an IRDA transceiver **60** associated with the PC **59** and the device **200**. The device **200** can upload all transaction records to the PC **59** for bookkeeping, and the PC **59** can download information onto the device **200**.

[0044] **FIGURE 13** illustrates an information updating embodiment of the present invention wherein the information stored within device **200** is updated via wireless transmission. An embodiment of this system does not require the user to have card reading/writing features associated with the device **200**. The network **95** in this example checks the user's card holder information as the user approaches a teller or greeting station, or an ATM. The network is wirelessly checking, for example, the expiration dates of the card accounts maintained by the user. The wireless transmission may be made via a variety of transmission systems, for example RF systems, IRDA systems, transponder systems, etc. Further, an additional service provided by the present system enables the customer to change the PIN via wireless transmission. The information downloading features are not limited to after-transaction usage of an ATM. The device **200** may be set to receive message downloading as the user comes within a predetermined range of an ATM or a bank branch. Additionally, the bank's network can deactivate a user's account when a user approaches an ATM or a branch location.

[0045] Embodiments of the present invention have now been described in fulfillment of the above objects. It should be appreciated that these examples are merely illustrative of the invention. Many variations and modifications will be apparent to those skilled in the art.

Claims

1. An information exchange device, comprising:

   a user interface for receiving input from a user to initiate an information exchange;
   a power source for providing power to enable standalone operation of said device;
   a central processing unit operatively connected to said user interface for controlling the operation of said device;
   a memory component operatively connected to said central processing unit, for storing information and software;
   an encryption/decryption processor for enabling encryption/decryption of data transmitted via a wireless data transmission;
   a communications module enabling, without said user's prompt, said wireless data transmission between said device and a terminal when said device is within a communications range of said terminal; and
   wherein said communications module wirelessly transmits verification information associated with an authorized user of said device to enable verification of whether said user of said device is said authorized user.

2. The information exchange device of Claim 1, wherein said terminal is a personal digital assistant.

3. The information exchange device of Claim 1, wherein said terminal is an automated teller machine.

4. The information exchange device of Claim 1, wherein said terminal is a greeting terminal wherein information received by said terminal is for customer service.

5. The information exchange device of Claim 1, further comprising:

   a card reader/writer; and
   a universal card wherein data is retrieved from and written onto said card by said card reader/writer and wherein said data on said universal card is eraseable.

6. The information exchange device of Claim 5, wherein said universal card is a smart card.

7. The information exchange device of Claim 6, wherein said universal card is a magnetic stripe card.

8. The information exchange device of Claim 1, wherein said verification information associated with said authorized user is biometric information.

9. The information exchange device of Claim 8, wherein said biometric information is an iris identification code.

10. The information exchange device of Claim 1, wherein said user interface includes an emergency aid feature.

11. The information exchange device of Claim 10, wherein said emergency aid feature provides access to an authorized user's health information.

12. The information exchange device of Claim 1, further comprising a cellular telephone.

13. The information exchange device of Claim 1, wherein said wireless data transmission is via radio frequency.

14. The information exchange device of Claim 1, wherein said user interface is a liquid crystal display/interface.

15. The information exchange device of Claim 1, wherein said device is encased in a protective cover segmented by at least two panels.

16. The information exchange device of Claim 1, wherein said device is a handheld device.

17. The information exchange device of Claim 5, further comprising:

   a card docking port for said universal card wherein said card docking port has lips that abut three sides of said universal card when said universal card is docked in said docking port.

18. The information exchange device of Claim 17, further comprising:

   a protective cover for said device wherein said protective cover is segmented by at least two panels; and
   wherein said card docking port is associated with a first panel and said user interface is

associate with another panel.

19. The information exchange device of Claim 1, wherein said user interface is a keypad.

20. An information and transaction processing system, comprising:

a portable communications device;
a card reader/writer associated with said portable communications device;
a universal card wherein data is written and retrieved from said card with said card reader/writer, and wherein data is automatically erased from said card at a timed interval;
a biometric identifier for verifying a user of said portable communications device; and
an information terminal for automatic data transmission with said portable communications device when said portable communications device is within a communications range with said information terminal.

21. An information and transaction processing system, comprising:

a device with a user interface for receiving input from a user to initiate an information exchange;
a power source for providing power to enable standalone operation of said device;
a central processing unit operatively connected to said user interface for controlling the operation of said device;
a memory component operatively connected to said central processing unit, for storing information and software;
an encryption/decryption processor within the device for enabling encryption/decryption of data transmitted via a wireless data transmission;
a terminal for communicating with said device;
a communications module enabling, without said user's prompt, said wireless data transmission between said device and said terminal when said device is within a communications range of said terminal; and
wherein said communications module wirelessly transmits verification information associated with an authorized user of said device to enable said terminal to verify whether said user of said device is said authorized user.

22. The information and transaction processing system of Claim 21, wherein said terminal makes biometric observations of said user and compares said observations to said verification information received from said device.

23. The information and transaction processing system of Claim 22 further comprising an iris identification camera associated with said terminal for making said biometric observations.

24. The information and transaction processing system of Claim 21 wherein said terminal is an automated teller machine.

25. The information and transaction processing system of Claim 24 wherein said device wirelessly transmits a preset transaction request to said automated teller machine.

26. The information and transaction processing system of Claim 25 wherein said automated teller machine transmits a transaction record to said device after processing said preset transaction request.

27. A method for performing an electronic transaction with an information and transaction processing system, comprising:

receiving transactional information from a device;
receiving verification information from said device;
verifying a user of said device corresponds with said verification information; and
transmitting and receiving data automatically with said device when said device is within a predetermined communications range.

28. The method of Claim 27 for performing an electronic transaction with an information and transaction processing system wherein verifying said user of said device involves biometric observations.

29. The method of Claim 28 for performing an electronic transaction with an information and transaction processing system wherein said verification information is an IrisCode.

30. The method of Claim 27 for performing an electronic transaction with an information and transaction processing system wherein said transactional information is encoded on a universal card.

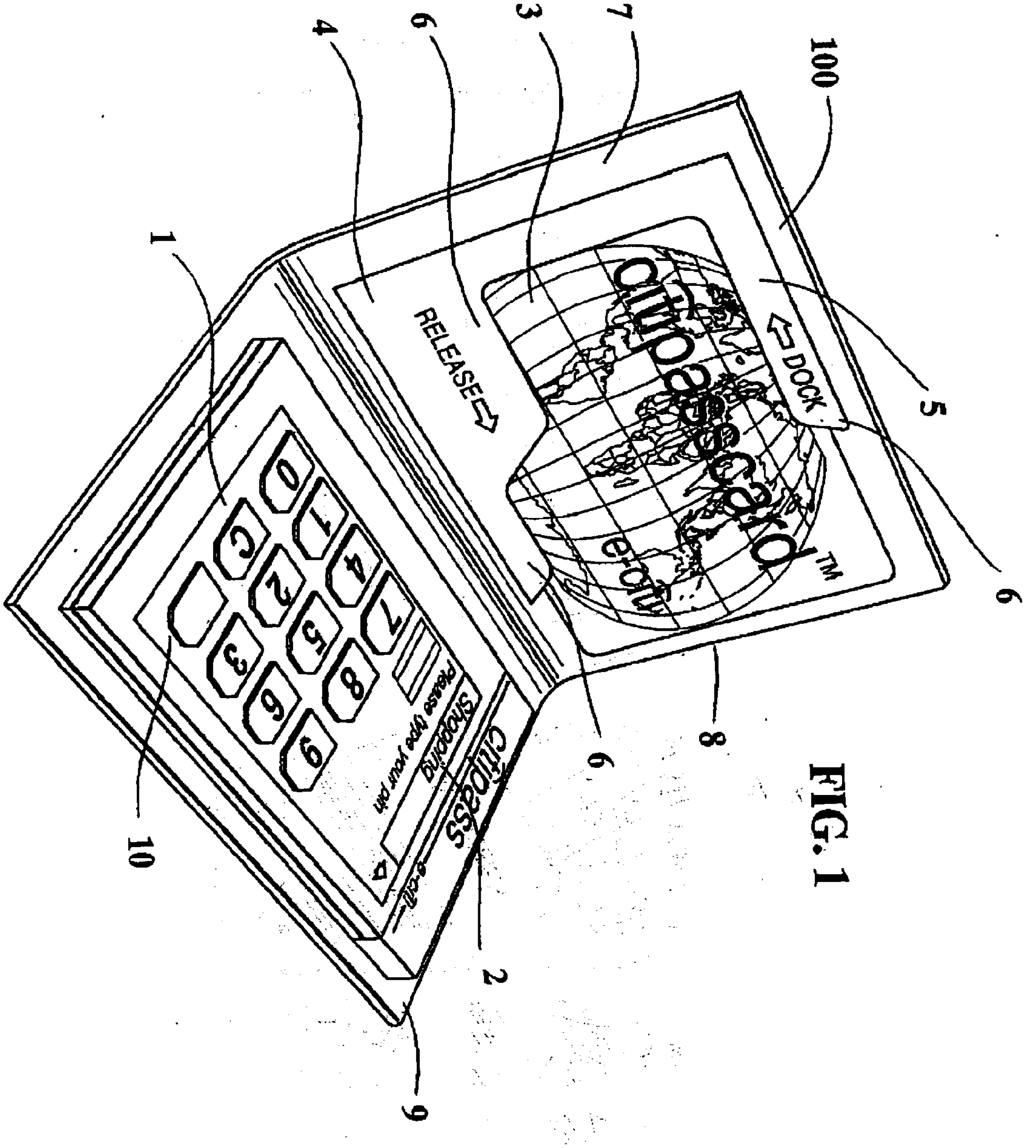

DOCK
RELEASE
citipasscard
TM
e-city
citipass
e-city
Shopping
Please type your pin
C

FIG. 1

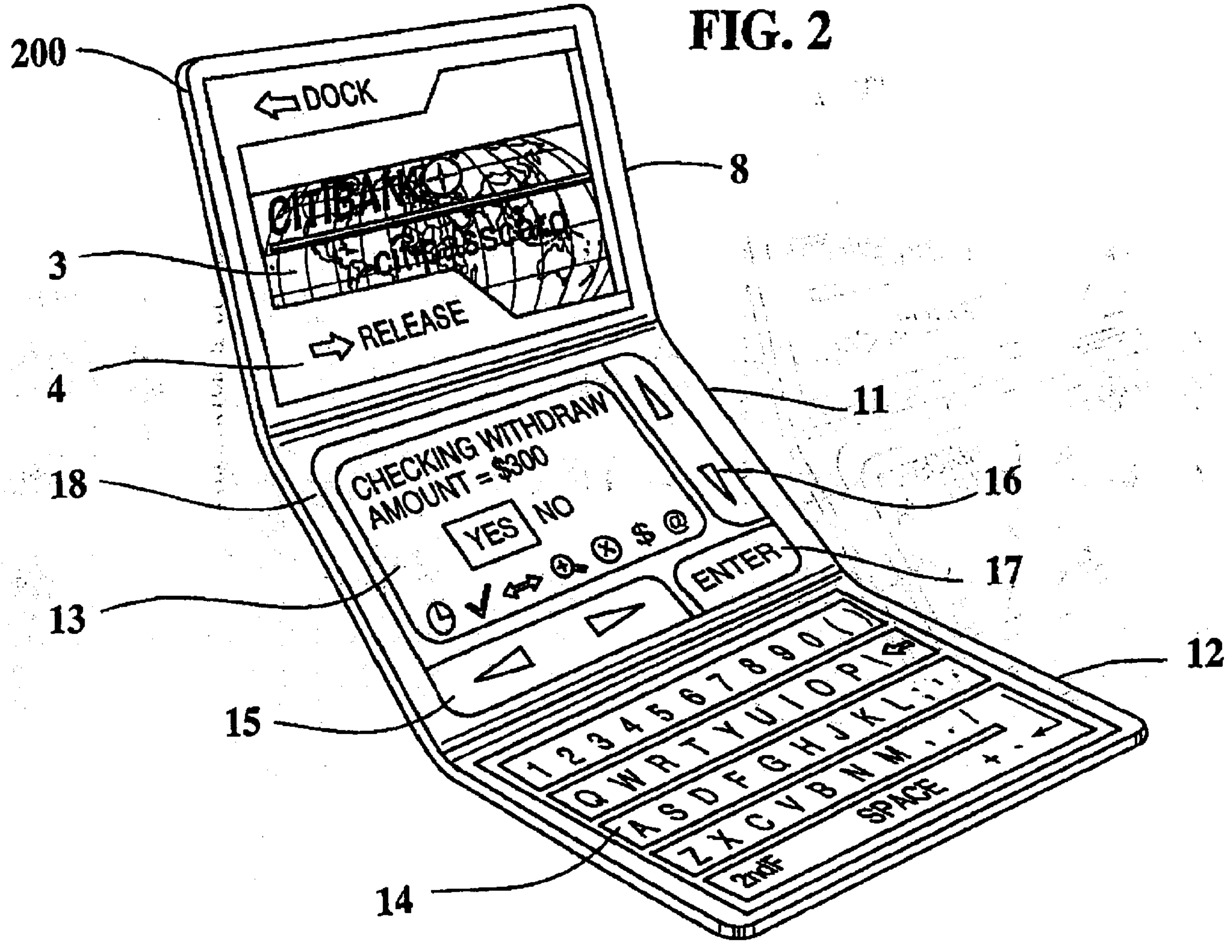

200
DOCK
CITIBANK
3
RELEASE
4
8
11
CHECKING WITHDRAW
AMOUNT = $300
YES
NO
$
@
18
13
16
ENTER
17
12
15
1 2 3 4 5 6 7 8 9 0 ( )
Q W R T Y U I O P \
A S D F G H J K L ; :
Z X C V B N M , . /
2ndF
SPACE
+ .
14

FIG. 2

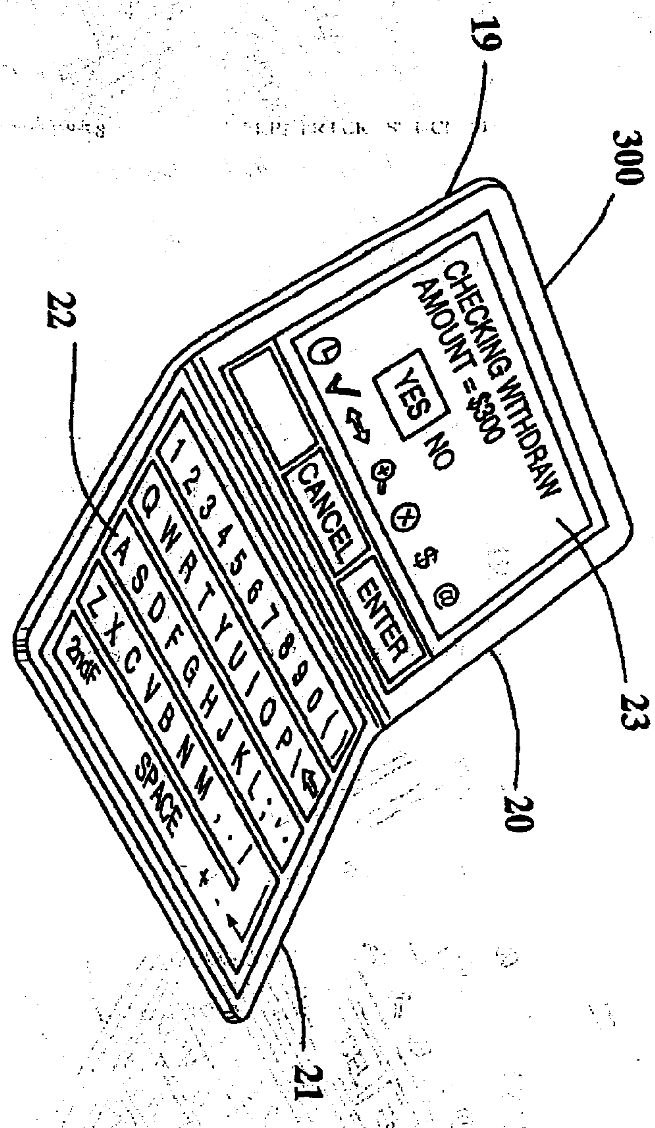

19
300
22
CHECKING WITHDRAW
AMOUNT = $300
YES
NO
$
@
CANCEL
ENTER
1 2 3 4 5 6 7 8 9 0
Q W R T Y U I O P
A S D F G H J K L ; :
Z X C V B N M , . /
2ndF
SPACE
23
20
21

FIG. 3

FIG. 4

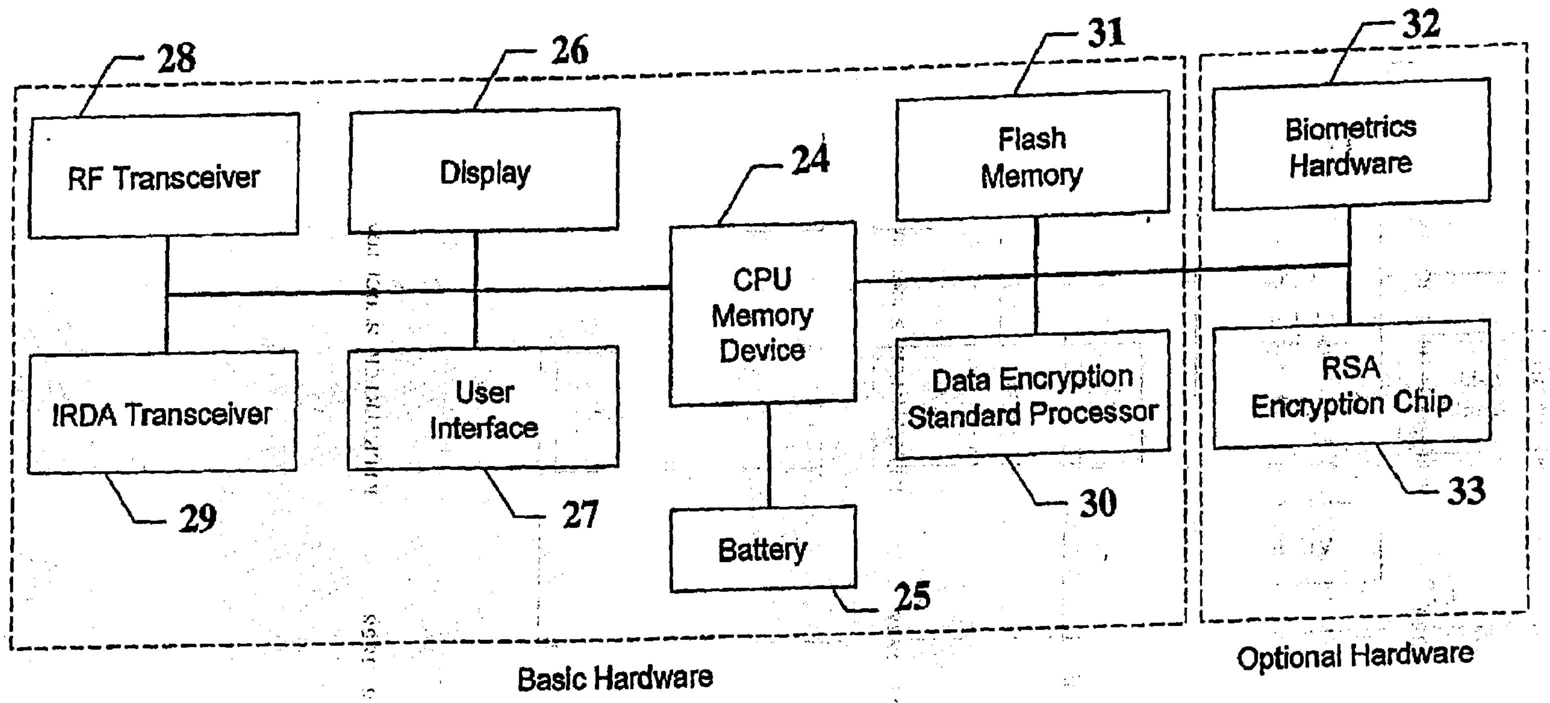
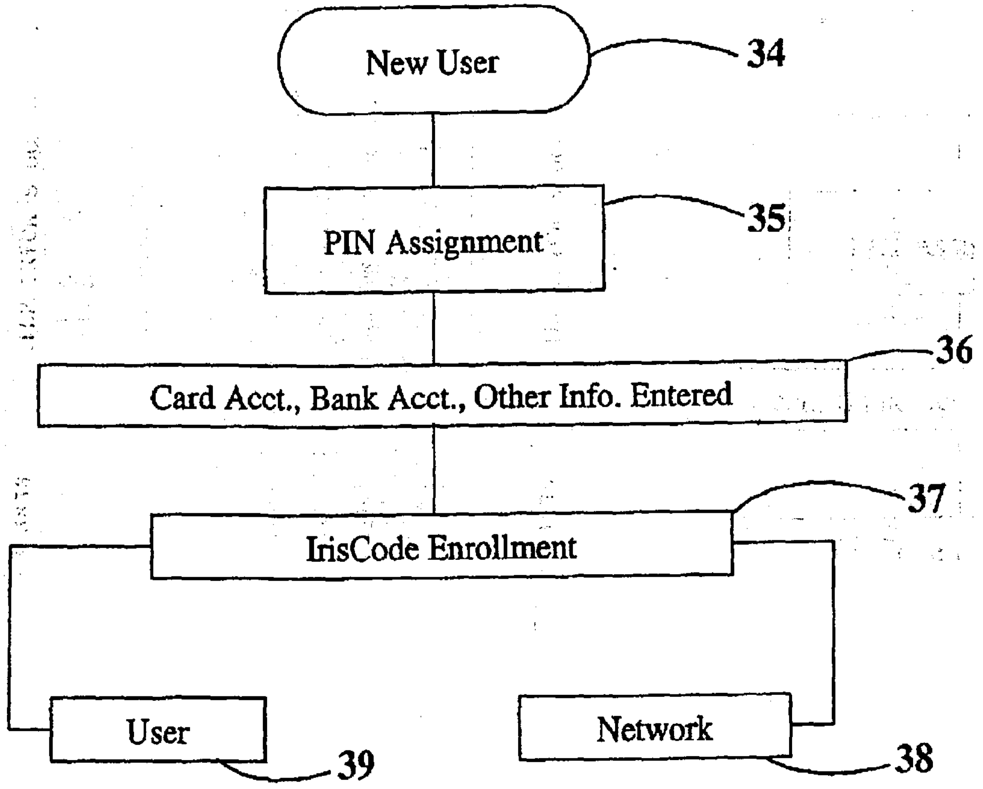

28
RF Transceiver
26
Display
24
CPU Memory Device
31
Flash Memory
32
Biometrics Hardware
IRDA Transceiver
29
User Interface
27
Battery
25
Data Encryption Standard Processor
30
RSA Encryption Chip
33
Basic Hardware
Optional Hardware

FIG. 5


New User
34
PIN Assignment
35
Card Acct., Bank Acct., Other Info. Entered
36
IrisCode Enrollment
37
User
39
Network
38

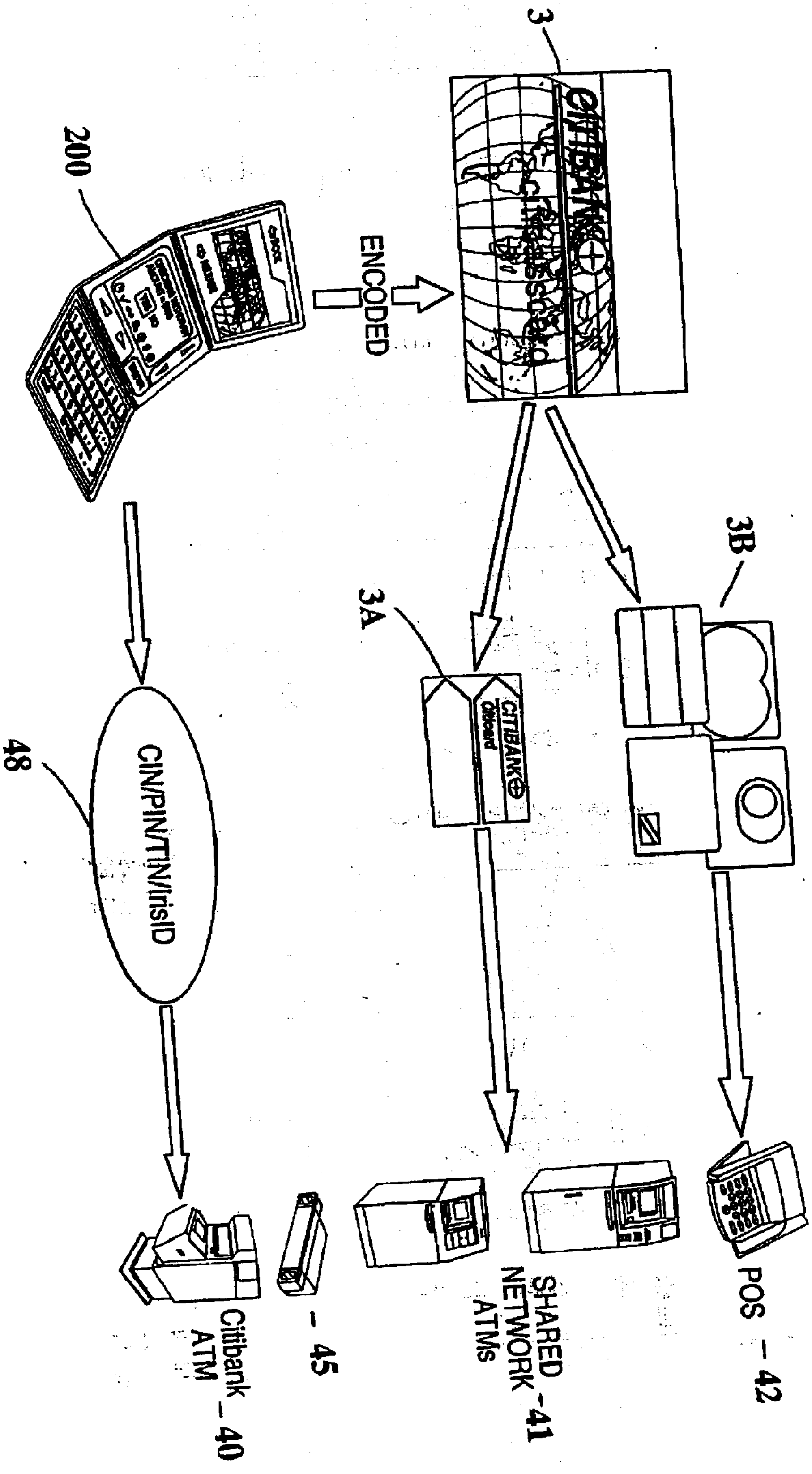

200
ENCODED
3
CITIBANK
3A
CITIBANK
Citicard
3B
48
CIN/PIN/TIN/IrisID
POS - 42
SHARED NETWORK ATMs -41
- 45
Citibank ATM - 40

FIG. 6

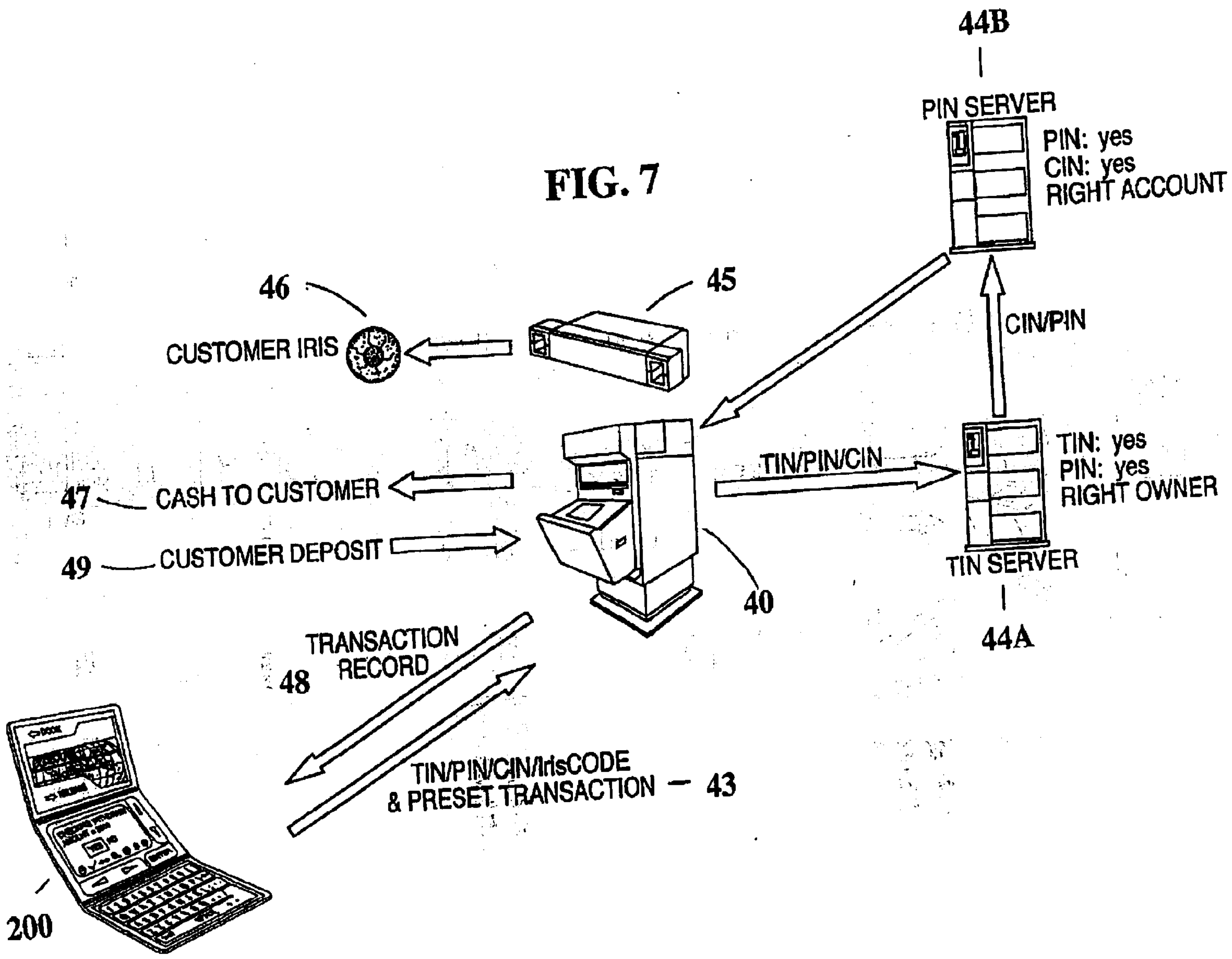

44B
PIN SERVER
PIN: yes
CIN: yes
RIGHT ACCOUNT
CIN/PIN
46
CUSTOMER IRIS
45
TIN/PIN/CIN
TIN: yes
PIN: yes
RIGHT OWNER
TIN SERVER
44A
47
CASH TO CUSTOMER
49
CUSTOMER DEPOSIT
40
TRANSACTION
RECORD
48
TIN/PIN/CIN/IrisCODE
& PRESET TRANSACTION
43
200

FIG. 7

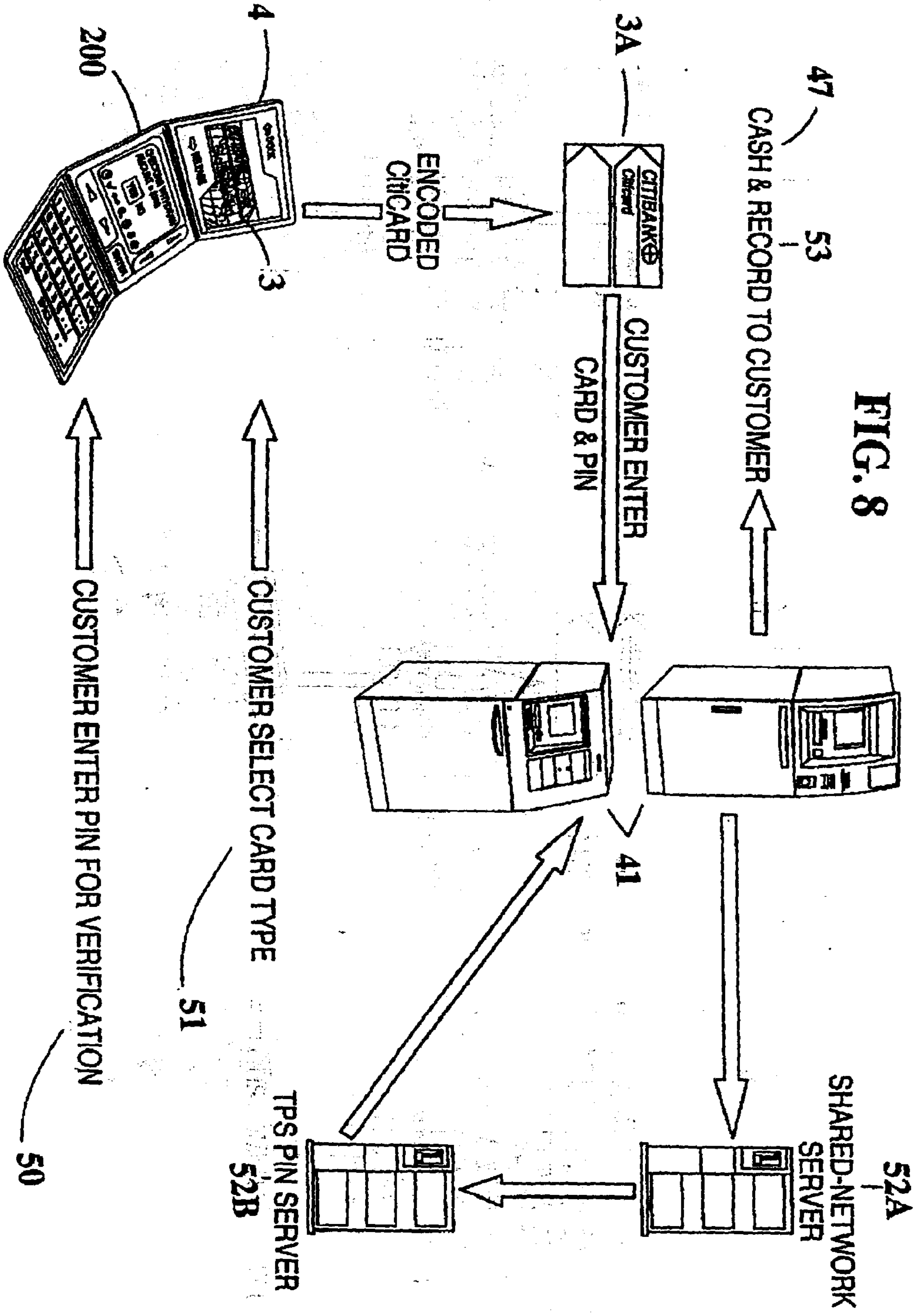

4
200
3
ENCODED CitiCARD
CITIBANK
Citicard
3A
47
CASH & RECORD TO CUSTOMER
53
CUSTOMER ENTER CARD & PIN
41
52A
SHARED-NETWORK SERVER
TPS PIN SERVER
52B
CUSTOMER SELECT CARD TYPE
51
CUSTOMER ENTER PIN FOR VERIFICATION
50

FIG. 8

FIG. 9

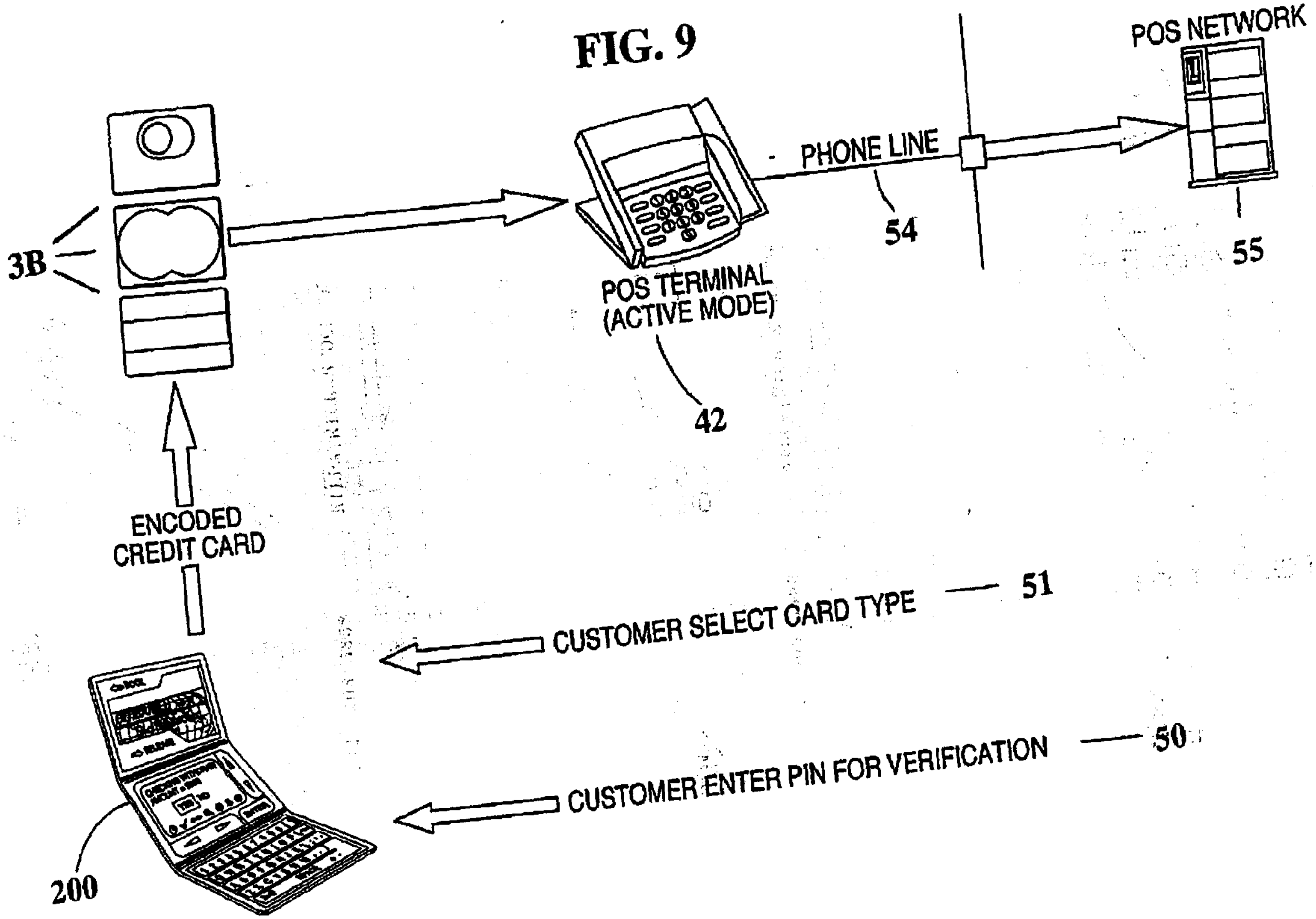

3B
POS NETWORK
PHONE LINE
54
55
POS TERMINAL
(ACTIVE MODE)
42
ENCODED
CREDIT CARD
CUSTOMER SELECT CARD TYPE
51
CUSTOMER ENTER PIN FOR VERIFICATION
50
200

FIG. 10

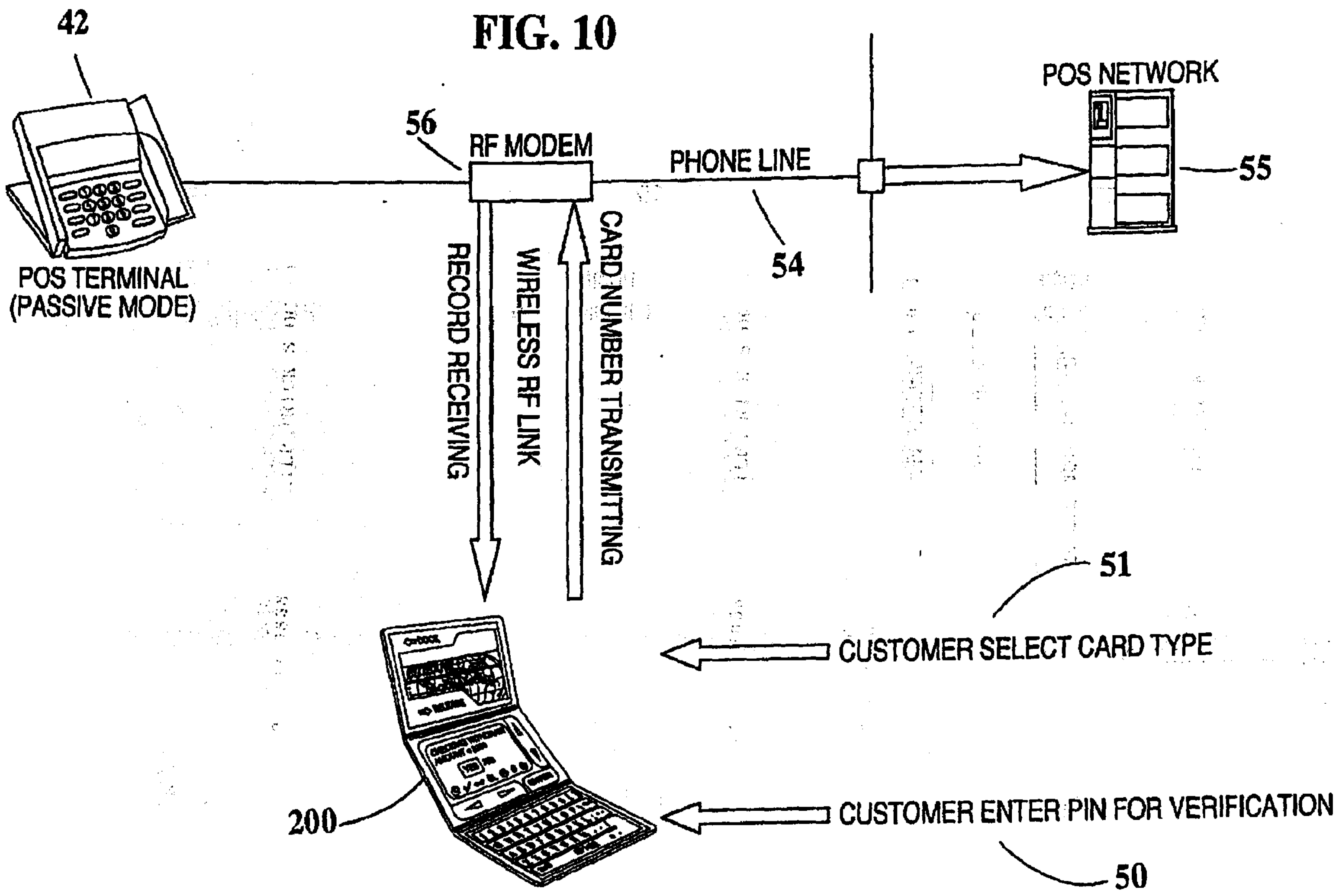
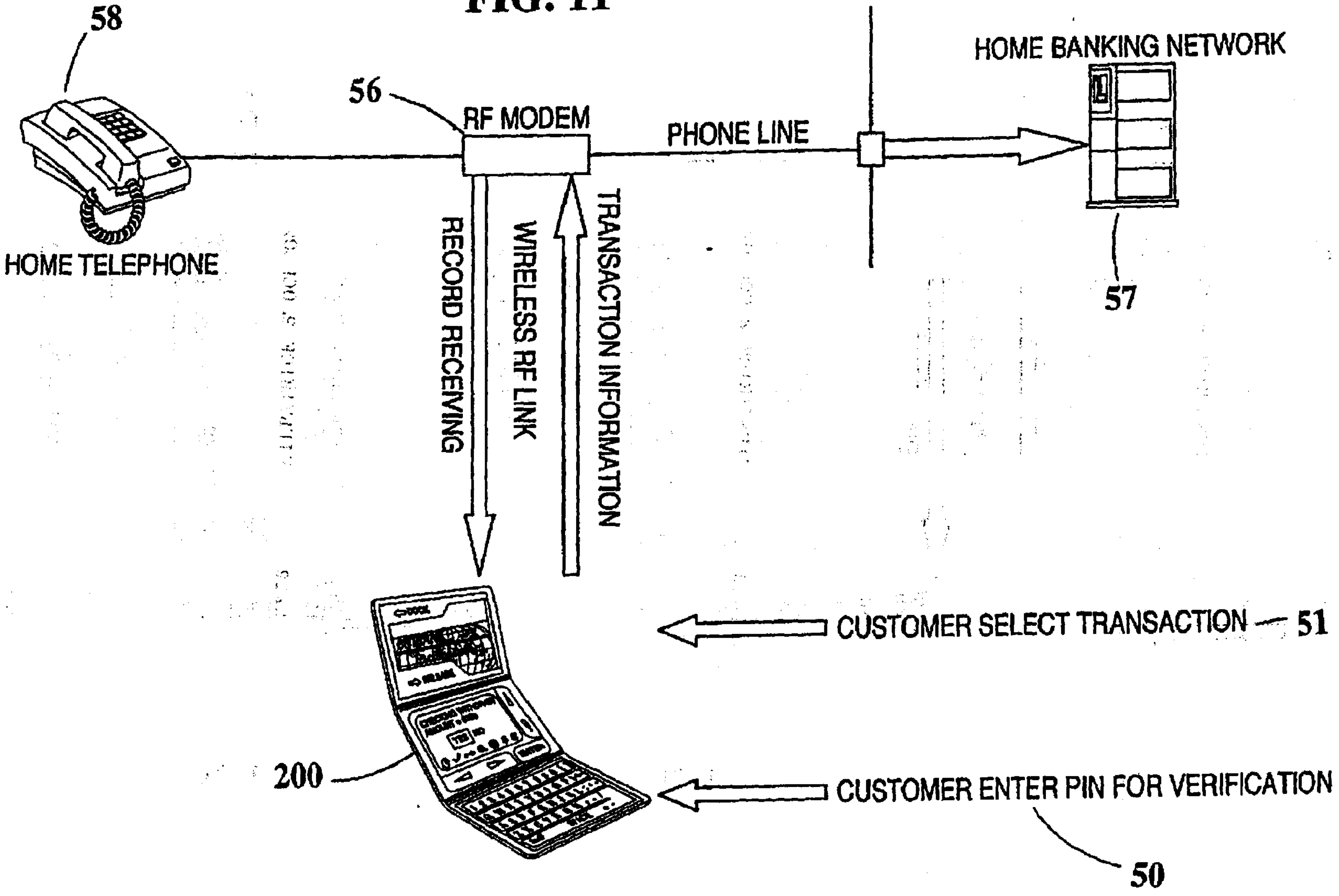

42
POS TERMINAL
(PASSIVE MODE)
56
RF MODEM
PHONE LINE
54
POS NETWORK
55
RECORD RECEIVING
WIRELESS RF LINK
CARD NUMBER TRANSMITTING
51
CUSTOMER SELECT CARD TYPE
200
CUSTOMER ENTER PIN FOR VERIFICATION
50

FIG. 11


58
56
RF MODEM
PHONE LINE
HOME BANKING NETWORK
HOME TELEPHONE
57
RECORD RECEIVING
WIRELESS RF LINK
TRANSACTION INFORMATION
CUSTOMER SELECT TRANSACTION
51
200
CUSTOMER ENTER PIN FOR VERIFICATION
50

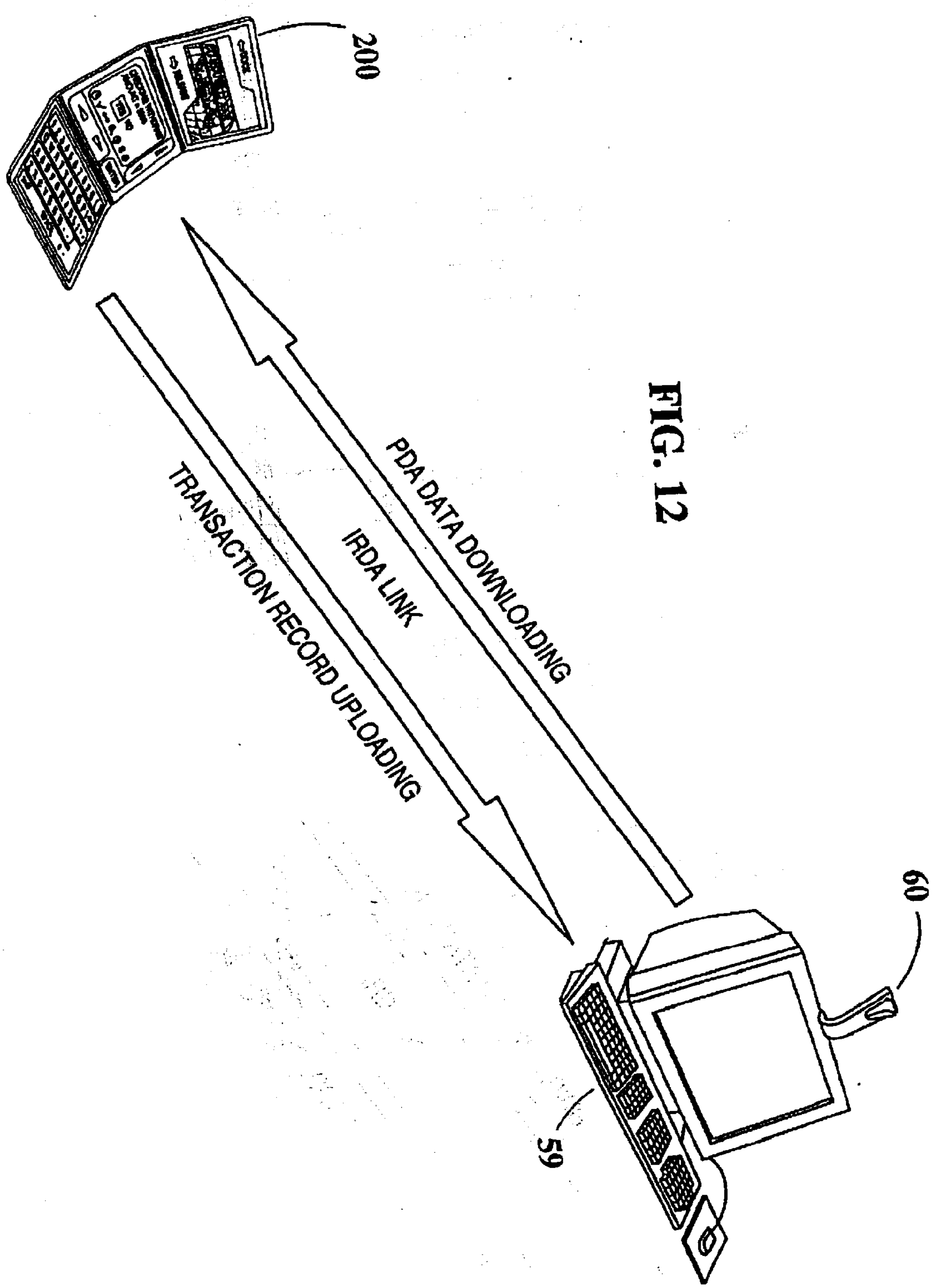
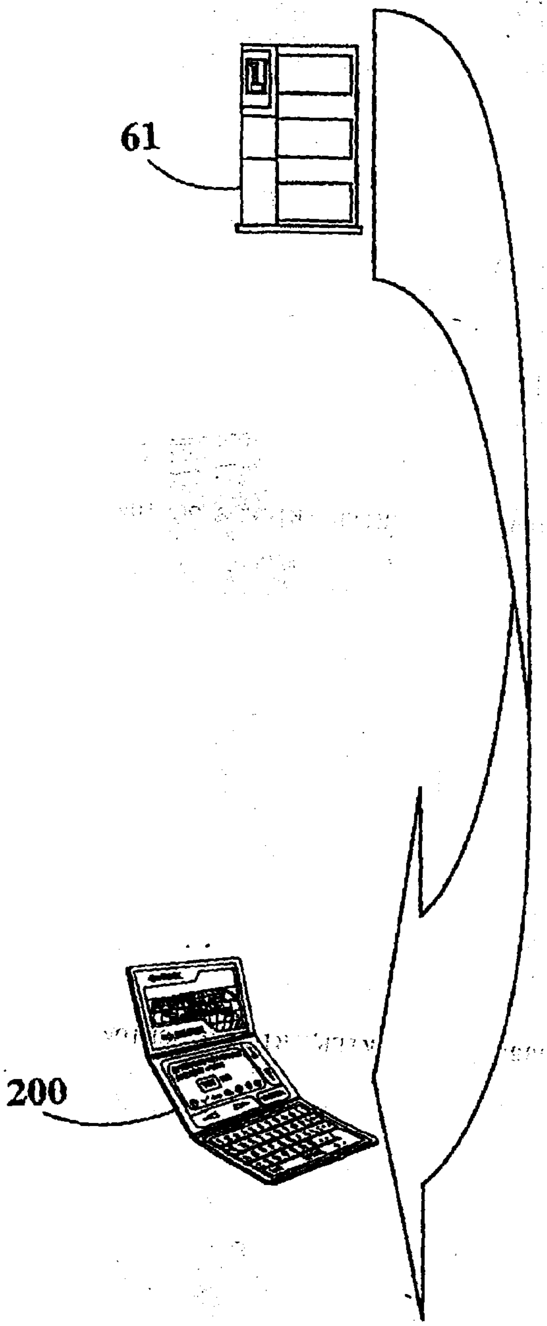

200
PDA DATA DOWNLOADING
IRDA LINK
TRANSACTION RECORD UPLOADING
60
59

FIG. 12

FIG. 13



European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 00 20 2089

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
X	WO 99 08238 A (IBM UK ;IBM (US)) 18 February 1999 (1999-02-18)	1-3,5-9, 12,13, 16,17, 19, 21-24, 27-30	G07F7/10
	* the whole document *		
Y		14,15,18	
A		10,11	

Y	US 5 319 582 A (MA HSI K) 7 June 1994 (1994-06-07) * figure 1 * * column 1, line 46 - column 2, line 5 *	14,15,18	

TECHNICAL FIELDS SEARCHED (Int.Cl.7)

G07F
G06K
G06F

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	28 September 2000	Lindholm, A-M

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 00 20 2089

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report.
The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

28-09-2000

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9908238 A	18-02-1999	US 6016476 A	18-01-2000
		EP 1004099 A	31-05-2000
US 5319582 A	07-06-1994	CN 2103831 U	06-05-1992

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82